COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, CHAIRMAN

MEDIA ADVISORY

For Immediate Release
June 6, 2006

Contact: Robert White
(202) 225-5074

Davis To Examine Security of Personal Data At Federal Agencies

In Light of Data Breach at Veterans Affairs, Committee Will Look at Security of Sensitive Personnel Info Across Government

What: **Government Reform Committee Oversight Hearing, "Once More Into the Data Breach: The Security of Personal Information at Federal Agencies"**

When: **THURSDAY, June 8, 2006, 10:00 A.M.**
(Hearing will immediately follow a business meeting.)

Where: **ROOM 2154, RAYBURN HOUSE OFFICE BUILDING**

Background: It is often said that we live in a digital world. That holds true for the federal government, too.

Government operations are dependent on information technology. E-commerce, information sharing, and Internet transactions, such as online tax filing, are commonplace. With the government's aggressive push to advance e-government initiatives, many government information systems hold personal information about millions of citizens and employees.

On May 3, 2006, an analyst with the Veterans Affairs Department reported personal computer equipment stolen in a home burglary. The computer equipment contained personal information about 26.5 million veterans that the employee had downloaded in order to work at home (although not as a part of an authorized telework program).

The data loss at VA is the largest by a federal agency to date, and the latest in a long string of personal information breaches in the public and

private sectors, including financial institutions, data broker companies, and academic institutions.

But the VA is far from alone. Just recently, a laptop computer containing information on 291 IRS employees and job applicants – including data such as fingerprints, names, Social Security numbers, and dates of birth – was lost while in transit on an airline flight, MSNBC reported.

These security breaches illustrate not only the risks associated with collecting and disseminating large amounts of electronic personal information, but the risk of harm or injury to consumers from identity theft crimes. The recent publicity surrounding these breaches has brought a new focus on establishing security standards for safeguarding customer information and imposing security breach notification obligations on entities that aggregate, possess, or license sensitive personal information

The Federal Information Security Management Act of 2002 (FISMA) requires federal government agencies to provide information security protections for agency information and information systems to provide integrity, confidentiality, and availability. FISMA requires each agency to create a comprehensive risk-based approach to agency-wide information security management. It is intended, in part, to make security management an integral part of an agency's operations. Chairman Davis was the chief sponsor of the FISMA legislation.

Each year, the Committee releases scorecards based on the information provided by agency Chief Information Officers and Inspectors General in their FISMA reports. This year, the Committee's analysis revealed that the scores for many departments remained unacceptably low or dropped precipitously.

The Veterans Affairs Department scored an F on this year's FISMA scorecard, the second consecutive year and fourth out of five the department receiving a failing grade. The federal government overall received a D+ grade, although several agencies improved their information security or maintained a consistently high level of security from previous years, including the Office of Management and Budget and the Social Security Administration.

The hearing will examine the government-wide efforts to improve data security. It will also specifically focus on security at Veterans Affairs, the Social Security Administration, and the IRS. VA Secretary Nicholson will discuss the details of that agency's data breach, while officials from the IRS and SSA will discuss the efforts of those agencies, which contain the largest storehouses of taxpayer information.

Witnesses:

Clay Johnson III, Deputy Director for Management, Office of Management and Budget
David M. Walker, Comptroller General of the United States, U.S. Government Accountability Office
R. James Nicholson, Secretary, Department of Veterans Affairs
William E. Gray, Deputy Commissioner for Systems, Social Security Administration
Daniel Galik, Chief Mission Assurance and Security Services, Internal Revenue Service, Department of Treasury

# # # # #